

# Analisis Yuridis Pencurian Data pada Waktu *Work From Home* (WFH) di Masa Pandemi Covid-19 Dihubungkan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Geraldint Feisal Rosidin, Nandang Sambas

Prodi Ilmu Hukum, Fakultas Hukum

Universitas Islam Bandung

Bandung, Indonesia

Geraldint1998@yahoo.com, nandangambas@yahoo.com

**Abstract**— Advances in technology, especially computers and the internet, cannot be separated from human life. All forms of information have become a "Power" which is defined as something that can determine the fate of humans themselves. During the Work From Home (WFH) period during the Covid-19 pandemic, millions of people around the world have to leave the office, school, and do all their activities at home. Problems arise when the security of personal data is threatened when accessing all obligations and needs via the internet with weak security. The purpose of this study is to determine whether or not Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions can ensnare perpetrators of criminal acts of data theft and protect personal data of victims from crimes of personal data theft. The methodology used in writing this thesis is a normative juridical approach, descriptive analytical research specifications, methods and data collection techniques are literature studies, and the method used is qualitative juridical. The results of the study of several data theft cases that have occurred during the covid -19 pandemic, someone who steals personal data can be sentenced, for violating Article 26 paragraph (1) j.o Article 30 paragraph (3) j.o Article 32 of the ITE Law. Victims of criminal acts of theft of personal data get legal protection from the ITE Law and the Regulation of the Minister of Communication and Information. This shows that the Information and Electronic Transaction Law can still contribute to enforcement and protection, but this is still considered ineffective, it is deemed necessary to ratify a separate law relating to the protection of personal data so as to provide security guarantees and protection of personal data.

**Keywords**— *DataTheft, Work From Home, Covid-19 Pandemi*

**Abstrak**— Kemajuan teknologi terutama pada komputer serta internet tidak dapat dipisahkan di kehidupan manusia. Segala bentuk informasi sudah menjadi suatu "Kekuatan" yang diartikan sebagai sesuatu yang dapat menentukan nasib manusia itu sendiri. Pada Masa Work From Home (WFH) di

saat pandemi Covid-19 ini memaksa jutaan orang diseluruh dunia meninggalkan kantor, sekolah, dan melakukan segala kegiatannya dirumah. Permasalahan muncul ketika kemanan atas data pribadi terancam ketika mengakses segala kewajiban dan kebutuhan melalui internet dengan keamanan yang lemah. Tujuan penelitian ini untuk mengetahui bisa atau tidaknya Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menjerat para pelaku tindak pidana pencurian data dan melindungi data pribadi para korban dari kejahatan pencurian data pribadi. Metodologi yang digunakan dalam penulisan skripsi ini adalah pendekatan yuridis normatif, spesifikasi penelitian deskriptif analitis, metode dan Teknik pengumpulan data adalah studi kepustakaan, serta metode yang digunakan berupa yuridis kualitatif. Hasil dari penelitian beberapa kasus pencurian data yang sudah terjadi selama pandemi covid -19, seseorang yang mencuri data pribadi dapat dijatuhi hukuman, karena melanggar pasal 26 ayat (1) j.o Pasal 30 ayat (3) j.o Pasal 32 UU ITE. Para korban dari tindak pidana pencurian data pribadi mendapatkan perlindungan hukum dari UU ITE dan Peraturan Menteri Komunikasi dan Informatika. Ini Menunjukkan bahwa UU Informasi dan Transaksi Elektronik masih bisa berkontribusi untuk melakukan penegakan dan perlindungan, namun hal ini masih dianggap kurang efektif, hal ini dipandang perlu disahkan undang-undang tersendiri yang berkaitan dengan perlindungan data pribadi sehingga memberikan jaminan keamanan dan perlindungan data pribadi.

**Kata Kunci**— *Pencurian Data, Work From Home, Pandemi Covid-19*

## I. PENDAHULUAN

Indonesia merupakan negara hukum hal ini diatur dalam Pasal 1 ayat (3) UUD 1945. Hukum berfungsi untuk mengatur hubungan antara manusia yang satu dengan manusia yang lainnya dan hubungan antara manusia dan negara agar segala sesuatunya berjalan dengan tertib

Awal Tahun 2019, kantor Organisasi Kesehatan Dunia (WHO) di China mendapatkan pemberitahuan tentang adanya sejenis penyakit Pneumonia yang penyebabnya tidak diketahui. COVID 19 menyebar ke seluruh dunia silih berganti dengan cara penularan yang disebut kasus import dari luar wilayah asal atau transmisi lokal antar penduduk. COVID 19 menyebar ke seluruh dunia silih berganti dengan cara penularan yang disebut kasus import dari luar wilayah asal atau transmisi lokal antar penduduk. Di seluruh dunia jutaan orang telah meninggalkan kantor menyusul instruksi pemerintah agar karyawan bekerja dari rumah (*work from home*).

Seiring waktu berjalan teknologi terutama pada komputer serta internet tidak dapat dipisahkan di kehidupan manusia. Dibalik kelebihan dan kemudahan yang diberikan oleh komputer serta internet, ternyata memiliki sisi gelap yang kemudian mampu menghancurkan kehidupan manusia itu sendiri. Pada masa pandemi Covid-19 ini keterbutuhan terhadap teknologi informasi semakin tinggi sehingga resiko yang dihadapi akan semakin tinggi. Perkembangan teknologi menjadi “pedang bermata dua” karena selain memberikan kontribusi seperti disaat pandemi seperti kemudahan mengakses pekerjaan tanpa harus pergi kemanapun, sekaligus menjadi sarana efektif perbuatan melawan hukum termasuk tindak pidana kejahatan seperti pencurian data.

Suatu kejahatan atau tindak pidana, umumnya dilakukan pelaku karena didorong atau dimotivasi oleh pemenuhan kebutuhan hidup yang relative sulit dipenuhi. Kemajuan ilmu pengetahuan dan teknologi yang tinggi seperti ini ditambah dengan kondisi pandemi Covid-19 memberikan peluang tindak kejahatan semakin tinggi dari volume hingga kualitas tindak pidana makin bervariasi seperti dalam kasus pencurian data.

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini sebagai berikut: 1. “Apakah Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dapat menjerat pelaku pidana pencurian data yang dilakukan pada *waktu work from home* di masa pandemi covid 19?”. 2. “Bagaimanakah bentuk perlindungan hukum yang diberikan kepada pemilik data yang menjadi korban tindak pidana pencurian data selama *work from home* di masa pandemi covid 19 ditinjau dari Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik?”. Tujuan dalam penelitian ini adalah Untuk mengetahui dapat atau tidaknya Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menjerat pelaku pidana pencurian data dan untuk mengetahui bentuk perlindungan hukum yang diberikan kepada korban dari tindak pencurian data menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

## II. LANDASAN TEORI

Istilah tindak pidana pada dasarnya merupakan terjemahan dari bahasa Belanda *Strafbaar feit* yang memiliki banyak istilah lain yaitu delik, peristiwa pidana, perbuatan pidana, perbuatan-perbuatan yang dapat dihukum, hal yang diancam dengan hukum, perbuatan-perbuatan yang diancam dengan hukum. Tindak pidana menurut Bambang Poernomo, yaitu perbuatan yang dilakukan oleh seseorang dengan melakukan suatu kejahatan atau pelanggaran pidana yang merugikan kepentingan orang lain atau merugikan kepentingan umum.

Kejahatan pencurian adalah salah satu kejahatan terhadap kepentingan individu yang merupakan kejahatan terhadap benda/kekayaan. Hal ini termuat dalam Bab XXII Pasal 362-367 KUH Pidana.

Indonesia sebagai negara modern tentu memerlukan teknologi dan informasi dalam mengikuti perkembangan ekonomi. Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, tetapi munculnya era komputer menciptakan ancaman yang lebih besar bagi privasi individu tersebut, serta kemungkinan individu menderita kerugian sebagai akibat dari ketidaktelitian atau pembocoran informasi akan jauh lebih besar. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik pada Pasal 1 ayat (1) menjelaskan Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiannya. Pasal 1 ayat (3) dikatakan bahwa pemilik data pribadi adalah individu yang padanya melekat Data Perseorangan Tertentu.

Pencurian data adalah tindak kriminal dalam dunia internet, dimana akan ada penyusup masuk kedalam data pribadi seseorang lalu mengambilnya tanpa izin. Data yang telah diambil digunakan oleh penyusup untuk berbagai macam kejahatan. Berbagai cara yang diambil penyusup untuk mengambil data tersebut, hal ini telah dibuktikan bahwa dibalik lalu lintas internet, banyak penyusup yang mencari celah untuk mengambil data tersebut. Data yang mereka incar adalah data yang cukup penting, misalnya data negara. Oleh karena itu, seorang ahli IT jaringan haruslah lihai untuk menyembunyikan data tersebut agar tidak adanya penyusup yang masuk ke dalam data.

Dalam suatu perlindungan data pribadi dikenal prinsip-prinsip yakni pembatasan pengumpulan, kualitas data, spesifikasi tujuan, penggunaan pembatasan, langkah-langkah pengamanan, keterbukaan, partisipasi individu, serta pertanggungjawaban.

Menurut Setiono, Perlindungan Hukum adalah tindakan atau upaya untuk melindungi masyarakat dari perbuatan sewenang-wenang oleh penguasa yang tidak sesuai dengan aturan hukum, untuk mewujudkan ketertiban dan ketentraman sehingga memungkinkan manusia untuk menikmati martabatnya sebagai manusia.

Menurut Bambang Waluyo dalam bukunya yang berjudul *Viktimologi Perlindungan Korban dan Saksi*,

bahwa yang dimaksud dengan korban adalah “orang yang telah mendapat penderitaan fisik atau penderitaan mental, kerugian harta benda atau mengakibatkan mati atas perbuatan atau usaha pelanggaran ringan dilakukan oleh pelaku tindak pidana dan lainnya”. Disini jelas yang dimaksud “orang yang mendapat penderitaan fisik dan seterusnya” itu adalah korban dari pelanggaran atau tindak pidana.

Penegakan hukum adalah proses dilakukannya upaya untuk tegaknya atau berfungsinya norma-norma hukum secara nyata sebagai pedoman perilaku dalam lalu lintas atau hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara. Ditinjau dari sudut subyeknya, penegakan hukum itu dapat dilakukan oleh subyek yang luas dan dapat pula diartikan sebagai upaya penegakan hukum itu melibatkan semua subyek. Penegakan hukum adalah suatu usaha untuk mewujudkan ide-ide tentang keadilan-keadilan, kepastian hukum dan kemanfaatan sosial menjadi kenyataan.

### III. HASIL PENELITIAN DAN PEMBAHASAN

#### A. *Pencurian Data Pada Waktu Work From Home Di Masa Pandemi Covid-19 Dihubungkan Dengan Undang-Undang Informasi Dan Transaksi Elektronik*

Dari awal mula covid-19 menyebar dan disaat work from home mulai diberlakukan sudah terjadi 11 kasus pencurian data pribadi di Indonesia selama penelusuran penulis lakukan, yaitu : 1. Kasus Tokopedia 2 Mei 2020, tentang Pencurian 91 Juta Data Pengguna, 2. Pencurian Data Pengguna Bhineka.com, 10 Maret 2020, 3. KreditPlus, Terkait Kebocoran Data Pengguna, 8 Mei 2020, 4. ShopBack, Data pengguna bocor 27 September 2020, 5. RedDoorz, Bocor: Nama, Nomor Telepon, Hingga Email 27 September 2020, 6. 2,9 Juta Data Pengguna Cermati.com Dikabarkan Dicuri Hacker, 11 April 2020, 7.

Lazada Kebobolan, 1,1 Juta Data Pengguna RedMart Diretas, 29 Oktober 2020, 8. 230 Ribu Data Pasien Covid-19 di Indonesia Bocor dan Dijual, 20 Mei 2020, 9. Pelaku Pembobolan Data Pelanggan Telkomsel Ditangkap Polisi, 10. Ratusan Aplikasi Android Curi Data Selama Pandemi Corona, Januari 2020, 11. 500 Juta Data Pengguna LinkedIn Bocor, Dilelang Mulai Rp.29.000, 9 April 2021.

Bentuk kewajiban yang harus dipenuhi oleh e-commerce agar data pribadi terjamin kemannya dan perlindungan hukum untuk korban selama ini berpegang kepada Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut “UU ITE”), meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses ilegal. Terkait penanggulangan pencurian data pribadi melalui sarana penal yaitu dengan memberikan perlindungan kepada data pribadi dari penggunaan atau pemanfaatan tanpa izin.

Ketentuan Pasal 26 UU ITE adalah sebagai berikut : 1.

Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. 2. Setiap orang yang melanggar haknya sebagaimana yang dimaksud pada ayat 1 dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini. 3. Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan. 4. Setiap penyelenggara sistem elektronik wajib menyediakan mekanisme penghapusan informasi elektronik dan/atau dokumen elektronik yang tidak relevan sesuai dengan ketentuan peraturan perundang-undangan. 5. Ketentuan mengenai tata cara penghapusan informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah

Berdasarkan isi dari pasal tersebut artinya aktivitas-aktivitas seperti pengumpulan dan penyebarluasan data pribadi merupakan pelanggaran terhadap privasi seseorang karena hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi. Pada dasarnya ketentuan ini memuat dua dasar legitimasi pemrosesan data pribadi yaitu (a) consent/persetujuan; dan (b) norma hukum positif. Kedua prinsip ini adalah dasar lawful data processing.

Dalam UU ITE khususnya Pasal 26 pemerintah memberikan solusi ketika penyelenggara sistem elektronik tidak mematuhi atau melakukan pelanggaran yang berkaitan dengan data pribadi bisa mengajukan gugatan perdata kepada pengadilan atas pelanggaran yang dilakukan. Selain untuk mencegah pelanggaran penyalahgunaan berupa pencurian data pribadi pemerintah melalui UU ITE tersebut memberikan perintah kepada penyelenggaraan sistem elektronik untuk menyiapkan suatu sistem yang berorientasi melakukan penyesuaian dan penghapusan pada data pribadi yang dianggap sudah tidak sesuai berdasarkan permintaan dari pihak terkait kepada pengadilan dan putusan pengadilan. Tetapi keadaan penghapusan sebagaimana disebutkan masalah umum, dengan sekedar menyebutkan penghapusan informasi elektronik dan/atau dokumen elektronik yang tidak relevan. Tidak ada penjelasan yang detil mengenai informasi yang tidak relevan. Keadaan seperti ini berpotensi bertabrakan dengan beberapa perundang-undangan lain dalam penerapannya dikemudian hari.

Dari fakta lapangan tersebut diketahui Cracking dimaknai sebagai peretasan dengan cara merusak sebuah sistem elektronik. Selain merusak, cracking merupakan pembajakan data pribadi maupun account pribadi seseorang, sehingga mengakibatkan hilang atau berubah dan digunakan tanpa persetujuan pemilik. Oleh karena itu, penggunaan data pribadi oleh cracker dengan tujuan sebagaimana dimaksud di atas dapat dikategorikan sebagai bentuk pelanggaran Pasal 26 ayat (1) UU Nomor 19 Tahun

2016. Yaitu “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.”, Selanjutnya, tindakan cracking tersebut dapat dikatakan termasuk perbuatan dalam Pasal 30 ayat (3) UU ITE, yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.” Atas perbuatannya, cracker dapat dijerat pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800 juta.

Tindakan cracking yang memenuhi unsur yang dimaksud dalam Pasal 32 UU ITE, mengatur : “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.” Pelanggaran atas pasal tersebut dikenakan jerat hukum sebagaimana disebut dalam Pasal 48 UU ITE seperti yang sudah dijelaskan sebelumnya di atas.

Bentuk perlindungan terhadap data pribadi dibagi dalam dua bentuk, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data itu, baik data yang kasat mata maupun data yang tidak kasat mata. Bentuk perlindungan data yang kedua adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan pengrusakan terhadap data itu sendiri

Masyarakat yang ingin memperjuangkan haknya sebagai korban dari tindak pencurian data pribadi dapat mengajukan gugatan perdata melalui pengadilan negeri, sesuai ketentuan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 26 ayat (1) dan (2) UU No.19 Tahun 2016.

Perlindungan data pribadi dalam sebuah sistem elektronik di Undang-Undang ITE meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan intervensi ilegal. Pada intinya, penggunaan setiap data dan informasi di media elektronik yang terkait dengan data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan atau berdasarkan hukum positif (peraturan perundang-undangan). Pada dasarnya ketentuan ini memuat dua dasar legitimasi pemrosesan data pribadi yaitu (a) consent/ persetujuan; dan (b) norma hukum positif. Kedua prinsip ini adalah dasar lawful data processing.

Dalam ketentuan umum Peraturan Pemerintah PSTE pada Pasal 1 ayat (27) disebutkan bahwa “data pribadi

adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya.” Dalam defenisi ini selain terdapat penjelasan mengenai apa itu data pribadi, terdapat juga amanat perlindungan terhadap kerahasiaan dari data pribadi

Pemilik data pribadi, menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, berhak atas kerahasiaan data miliknya; berhak mengajukan pengaduan dalam rangka penyelesaian sengketa data pribadi; berhak mendapatkan akses untuk memperoleh historis data pribadinya; dan berhak meminta pemusnahan data perseorangan tertentu miliknya dalam sistem elektronik. Hal terkait hak ini diatur dalam Pasal 26 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016.

Jika terjadi sengketa dalam pengelolaan data pribadi atau terjadi kegagalan dalam perlindungan kerahasiaan data pribadi, Peraturan Menteri Komunikasi dan Informatika ini membuka ruang pengaduan kepada Menteri (Kominfo), untuk dilakukan proses penyelesaian secara musyawarah atau alternatif penyelesaian sengketa lainnya, atau jika kedua mekanisme tersebut tidak berhasil, dapat menggunakan mekanisme gugatan perdata di pengadilan.

#### IV. KESIMPULAN

Berdasarkan pembahasan dalam penelitian ini, peneliti menyimpulkan 1. Untuk saat ini UU ITE bisa menjerat para pelaku tindak pidana pencurian data dan pihak yang kurang bertanggung jawab dalam melindungi data pribadi para konsumen yang menjadi korban tindak pidana pencurian data. Penggunaan data pribadi oleh cracker dengan tujuan pembajakan data pribadi maupun account pribadi seseorang, sehingga mengakibatkan hilang atau berubah dan digunakan tanpa persetujuan pemilik. Sebagaimana dimaksud dapat dikategorikan sebagai bentuk pelanggaran Pasal 26 ayat (1) UU Nomor 19 Tahun 2016. Lalu tindakan cracking tersebut dapat dikatakan termasuk perbuatan dalam Pasal 30 ayat (3) UU ITE (Informasi dan Transaksi Elektronik) juga, karena sengaja dan tanpa hak atau melawan hukum mengakses sistem elektronik dengan cara apapun. Atas perbuatannya tindak kejahatan Cracking dapat dijerat pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp.800 Juta.

Masyarakat yang menjadi korban dari tindakan pencurian data pribadi dapat memperjuangkan haknya, menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, berhak atas kerahasiaan data miliknya; berhak mengajukan pengaduan dalam rangka penyelesaian sengketa data pribadi; berhak mendapatkan akses untuk memperoleh historis data pribadinya; dan berhak meminta pemusnahan data perseorangan tertentu miliknya dalam sistem elektronik. dan Para penyelenggara sistem elektronik dalam memberikan keamanan kepada data pribadi konsumen dalam sistem elektronik tentu mendapat perlindungan hukumnya untuk menjamin kerahasiaan, keutuhan, serta penggunaan dan pemanfaatannya yang harus dilakukan berdasarkan persetujuan dari pemilik data

pribadi tersebut. Hal terkait ini diatur dalam Pasal 26 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016. Setiap penyelenggaraan sistem elektronik wajib memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia data pribadi. Jika terjadi hal tersebut, Peraturan Menteri Komunikasi dan Informatika ini membuka ruang pengaduan kepada Menteri (Kominfo), untuk dilakukan proses penyelesaian secara musyawarah atau alternatif penyelesaian sengketa lainnya, atau jika kedua mekanisme tersebut tidak berhasil, dapat menggunakan mekanisme gugatan perdata di pengadilan.

## V. SARAN

Untuk pemerintah (Direktorat Jenderal Peraturan Perundang-Undangan Kementerian Hukum) dan DPR untuk melakukan pembahasan lebih lanjut mengenai Undang – Undang Perlindungan Data Pribadi karena saat era digital seperti ini Undang - Undang tersebut sangat dibutuhkan untuk menindak para pelaku tindak pidana pencurian data pribadi agar ditindak dengan landasan undang-undang yang lebih jelas, terlebih untuk memberikannya edukasi terhadap masyarakat secara menyeluruh agar memperingatkan untuk lebih peduli terhadap pentingnya perlindungan diri terhadap data pribadi sendiri saat mengakses segala aktivitas yang dilakukan di saat work from home karena tingkat keamanan yang lemah dalam mengakses segala sistem perkantoran dirumah akan menjadi sebuah peluang bagi para pelaku tindak kejahatan untuk memanfaatkan kesempatan tersebut untuk melakukan tindak kejahatan.

Untuk Pemerintah dalam memberikan perlindungan kepada masyarakat terlebih khususnya perlindungan data pribadi harus lebih tersirat jelas aksi perlingkungannya, karena payung hukum untuk perlindungan data pribadi saat ini masih menjadi rancangan undang-undang maka, perlindungan yang harus diberikan pemerintah kepada masyarakat adalah sigap dalam menanggapi dan cepat menyelesaikan persoalan para penyelenggara sistem elektronik yang gagal melindungi data pribadi pada konsumen yang menjadi korban, dan memberikan sanksi serta masukan kepada para penyelenggara sistem elektronik untuk meningkatkan keamanan sistemnya agar dilain waktu hal tersebut tidak terulang kembali, dan tingkatkan segala kewanaman siber di negeri agar tidak mudah diakses dengan mudah oleh para pelaku tindak kejahatan. Pentingnya pemerintah memberikan sebuah protokol dalam mengakses segala kegiatan perkantoran agar masyarakat menjadi lebih patuh dan merasa aman karena sudah melaksanakan protokol tersebut untuk kenyamanan dalam mengakses segala hal untuk memenuhi kewajiban sebagai pegawai.

## DAFTAR PUSTAKA

- [1] UUD 1945
- [2] Mochtar Kusumaatmadja, Fungsi dan Perkembangan Hukum

- Dalam Pembangunan Nasional, Bandung, Penerbit Binacipta, 1986.
- [3] Dara Sawitri, “Penggunaan Google Meet Untuk Work From Home di Era Pandemi Coronavirus Disease 2019 (Covid-19)” *Jurnal Prioritas : Jurnal Pengabdian Masyarakat*, Volume : 02, Nomor : 01, April 2020.
  - [4] Brisilia Tumulun, “Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008,” *Jurnal Lex Et Societatis* 6, No. 2 (2018).
  - [5] A. Aco Agus dan Sikawati, “Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar),” *Jurnal Supremasi*, Vol.10, N (2016).
  - [6] Mulyana W. Kusumah, *Clipping Service Bidang Hukum*, Majalah Gema, 1991.
  - [7] Paul Marrett, *Information Law in Practice: 2nd Edition*, MPG Books Ltd., Cornwall, 2002.
  - [8] Peraturan Menteri Komunikasi Nomor 20 Tahun 2016
  - [9] Pencurian Data di Dunia Maya, <https://www.kompasiana.com/agnesj0122/5dfbb336097f3650221c41a2/pencurian-data-di-dunia-maya> (diakses pada tanggal 02 April 2021 pada pukul 20.50)
  - [10] Sinta Dewi, *Cyber Law: Aspek Daa Privasi Menurut Hukum Internasional, Regional, dan Nasional*, PT Refika Aditama, Bandung, 2015.
  - [11] Setiono, *Supremasi Hukum*, Surakarta: UNS, 2004.
  - [12] Bambang Waluyo, *Viktimologi Perlindungan Korban dan Saksi*, Sinar Grafika, Jakarta, 2011.
  - [13] Satjipto Rahardjo, *Masalah Penegakan Hukum*, Bandung : Sinar Baru, 1987.
  - [14] Undang-Undang Informasi dan Transaksi Elektronik.
  - [15] Human Rights Committee General Comment No, *On the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988.
  - [16] Andrew pelealu, Tesis :”Perlindungan Hukum Atas Data Pribadi Konsumen Dalam Transaksi E-Commerce”, Yogyakarta : Universitas AtmaJaya Yogyakarta, 2018.
  - [17] Lia Sautunnida, “Urgensi Undang - Undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia”, *Kanun Jurnal Ilmu Hukum* , Vol.20, No.2, Agustus, 2018.
  - [18] Sugeng, “Hukum Telekomunikasi Indonesia”, Prenadamedia Group, Jakarta, 2020.
  - [19] KOMINFO Kulonprogo, “Jamin Perlindungan Data Pribadi, Kominfo beri sanksi terhadap Penyalahgunaan oleh Pihak Ketiga.” Diakses melalui <https://kominfo.kulonprogo.kab.go.id/detil/469/jamin-perlindungan-data-pribadi-kominfo-beri-sanksi-terhadap-penyalahgunaan-oleh-pihak-ketiga>, (diakses pada tanggal 26 Mei 2021 Pukul 00.16)
  - [20] Siti Yuniarti, “Perlindungan Hukum Data Pribadi di Indonesia”, *Jurnal BECOSS*, Vol.1, No. 1, 2019
  - [21] Khairunisa Kania, Ravena Dey. (2021). *Analisis Hambatan Pelaksanaan Eksekusi Pidana Mati pada Pelaku Tindak Pidana Peredaran Narkotika di Dalam Lembaga Pemasyarakatan Dihubungkan dengan Putusan Mahkamah Konstitusi Nomor 107/PUU-XIII/2015*. *Jurnal Riset Ilmu Hukum*. 1(1). 15-20